UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/668,109	09/22/2003	Ram Anati	36437	7640

67801 7590 03/19/2008
MARTIN D. MOYNIHAN d/b/a PRTSI, INC.
P.O. BOX 16446
ARLINGTON, VA 22215

EXAMINER	
RAHIM, MONJUR	

ART UNIT	PAPER NUMBER
4141	

MAIL DATE	DELIVERY MODE
03/19/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/668,109	**Applicant(s)** ANATI ET AL.	
	Examiner MONJOUR RAHIM	**Art Unit** 4141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☒ Claim(s) *2* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on *22 September 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *04/20/2007*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Detailed Action

1. **Claims 1-36** are pending.

2. **Claims 1-36** are rejected.

Specification

3. Applicant is reminded of the proper content of an abstract of the disclosure.

> The abstract should be directed to the entire disclosure.

4. The abstract of the disclosure is objected to because it should be in one paragraph. Correction is required. See MPEP § 608.01(b).

Claim Objections

5. **Claim 2** is objected to because of the following informalities: It recites acronym "WWW", rather than full definition (i.e. World Wide Web). Appropriate correction is required.

Claim 31 is objected to because of the following informalities: It recites acronym "FSK", rather than full definition (i.e. Frequency Shift Key). Appropriate correction is required.

Drawings

6. The drawings filed on 09/22/2003 have been accepted by the examiner.

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 18 -36 are rejected under 35 USC 101

As per **claim 18** the limitation “sending an encrypted datagram”, “comparing said datagram” “generating a binary validation" are all program per se and does not have any output and thus the claims are non-statutory.

As per **claim 19**, the limitation “receiving an authentication datagram”, “protecting said datagram “, “forwarding said datagram” are all program per se; there are no concrete output. Thus the claim non-statuary.

Claim 20 is rejected due to the dependency of claim 19.

As per **claim 21,** the limitation “providing a code”, “generating said code”, “destroying said seed”, “storing said code” are all program per s; there are no concrete output. Thus the claim is non-statuary.

Claim 22-23 are rejected due to the dependency of claim 21.

As per **claim 24,** the limitation “generating a one time code”, “passing on said datagram”, “receiving an authentication”, are all program per se; there are no concrete output. Thus the claim is non-statuary.

Claim 25 is rejected due to the dependency of claim 24.

As per **claim 26**, the limitation “receiving an acoustic signal”, “matching said datagram”, “validating said authentication”, are all software modules; there are no concrete output. Thus the claim is non-statuary.

Claims 27-30 are rejected due to the dependency of claim 26.

As per **claim 31,** the limitation “receiving an authentication”, “correlating said converted signal”, “integrating said correlation”, “determining if a signal is present” are all software modules; there are no concrete output. Thus the claim is non-statuary.

Claims 32-36 are rejected due to the dependency of claim 31.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-8, 17-31 are rejected under 35 U.S.C. 102(b) as being anticipated by Caputo et al. (US PAT No. 5546463), hereinafter Caputo.

As per **claim 1**, Caputo discloses:

- A method of authenticating, using an authentication server, the use of an authentication device over a communication network via an intermediate communication device, comprising (Caputo, Abstract);

- receiving an authentication datagram by said intermediate device (Caputo, col 2, lines 20-25, “transportable authenticating and encrypting device which includes an encryptor for encrypting data received by the device, an authenticator for authenticating use of the device by a user, and a modem for transmitting the data and for receiving the data over a data transfer path”), where “encryption data (self-contained data)” is the Datagram and “Authenticator” is the intermediate device, as claimed;

- protecting said datagram by said intermediate device, by at least one of changing, adding to, encrypting and signing of said datagram; and forwarding said datagram to said authentication server for authentication (Caputo, col 3, lines 33-37, “The authenticator is preferably a cryptographic means which identifies the authorized user by an authorized user identification such as a message authentication code or digital signature”)and (Caputo, col 3, lines 46-49, “Preferably, the compact authenticating and encryption device includes a means of detecting the modification of messages sent or received by message authentication codes or digital signatures"), where "detecting modification message", such as digitally signed and encrypted data used here, as claimed.

As per **claim 2**, claim 1 is incorporated and further Caputo discloses:

- **wherein said intermediate device comprises a vendor WW'W site** (Caputo, Abstract, "The invention can operate as an electronic "token" to uniquely identify the user to a network").

As per **claim 3**, claim 2 is incorporated and Caputo further discloses:

- **wherein protecting comprises adding a signature associated with said vendor to said datagram** (Caputo, col 3, lines 48-50, "FIG. 5B is a block diagram which depicts device and user authentication in conjunction with digital signatures"), where digital signature was added to protect the unwanted user, as claimed.

As per **claim 4,** claim 2 is incorporated and Caputo further discloses:

- **wherein protecting comprises encrypting said datagram**(Caputo, col 6, lines 7-12' "The data is authenticated by a plurality of authentication algorithms well known to the art, all of which process messages and produce an authenticator number or digital signature which is transmitted with the data for use in verifying its source and accuracy").

As per **claim 5,** claim 1 is incorporated and Caputo further discloses:

- **A method according to claim ł, wherein said intermediate device comprises a user computing device** (Caputo, Abstract).

As per **claim 6,** claim 5 is incorporated and Caputo further discloses:

- **wherein said computing device adds a time stamp to said datagram** (Caputo, col 7, lines 43-49, "FIG. 5B describes a device and user authentication.

In this case, the user's name and, optionally, PIN is signed (Block 71), along with a counter (or time and date) which indicates that the data sent can be identified as not having been sent previously").

As per **claim 7,** claim 5 is incorporated and Caputo further discloses:

- wherein said computing device adds a time stamp to said datagram (Caputo, Fig. 4b, Fig. 4c), where vendor gets the "time stamp, Transaction data, reg#, user matrix, from the user/purchaser. User matrix is the part of the datagram as mention before.

As per **claim 8,** claim 5 is incorporated and Caputo further discloses:

- wherein said computing device encrypts said datagram (Caputo, col 2, lines 20-23, "a transportable authenticating and encrypting device which includes an encryptor for encrypting data received by the device, an authenticator for authenticating use of the device by a user").

As per **claim 17**, claim 1 is incorporated and Caputo further discloses:

- wherein different communication paths are used for said authentication and for transaction details from a vendor to said authentication (Caputo, col 7-8, lines 62-67 and 1-2, "The two ports of the encrypting/authenticating device 10 described in FIG. 1 are connected in FIG. 3 to a network 20 and a computer or terminal 22... communications in which data transmitted from authenticated user is passed through the device in a single pass and sent in encrypted form to the network through the modem"), where 2 ports used to exchange data, as claimed.

As per **claim 18**, Caputo discloses:

- sending an encrypted datagram by secure computer communication from a vendor software to said remote authenticator; (Caputo, col 4, lines 32-37, "The device will not permit communications to proceed until such device and, optionally, the user, have been identified by the authenticator. The device also contains all of the cryptography required to protect the data using data encryption or message authentication or digital signatures or any combination thereof");

- **comparing said datagram or a hash thereof to a hash table at said server** (Caputo, col 7, lines 30-42, "Digital signatures are a form of authentication which differs from the symmetrical key technology described ... Digital Signature Standard and Secure Hash Algorithm").

- **generating a binary validation answer by said server without an associated explanation** (Caputo, col 6, lines 22-27, "the validation process consists of encrypting the data in block 106 in accordance with the standard and in the same way as was done in block 100 and then comparing the resulting authentication codes with the authentication code which was received 104").

Claim 19 is rejected under the same reason set forth of claim 18 and Caputo further discloses:

- **datagram includes a secret code and wherein said secret code exists only on said authentication device** (Caputo, col 6, lines 47-51, "The authenticity of the device will be determined by the presence of a secret or private key either contained within the device itself or within a smartcard inserted into the device"), where "secret key" is the secret code, as claimed.

As per **claim 20**, claim 19 is incorporated and further Caputo discloses;

- **wherein said authentication device includes a plurality of secret codes that are generated to appear unrelated** (Caputo, col 8, lines 47-50, "Each of these algorithms employ a secret or private key to perform a cryptographic process upon the items listed above and produce an authenticator code or digital signature. The key 54 used to perform this authentication is held secret so as to prevent others from counterfeiting this code or signature").

As per **claim 21**, Caputo discloses:

- A method of generating a code set for an authentication device, comprising (Caputo, col 2, lines 46-49, “the compact authenticating and encryption device includes a means of detecting the modification of messages sent or received by message authentication codes or digital signatures”);

- providing a code generating software (Caputo, col 3, line 30, “encryption and authentication services can be provided for software application”);

- providing at least one seed code for said software (Caputo, col 5, lines 49-63, “The data is received (Block 80) and sent to a decryption function using a decryption algorithm which corresponds to the encryption algorithm described above and which recovers at output 84 the original plaintext 72"), where, “recovering output in original text” is the source code, as claimed;

- destroying said seed immediately after generating said code set (Caputo, 23-28, “the encrypted response sent by 70 is used in this transaction, then the comparison will, with virtual certainty, fail. The result of this comparison may be used by the challenger to terminate the communications session and alert a security officer that an unauthorized device”), where terminating call for the security reason is the same mechanism as claimed;

- storing said code set or an indication thereof on an authentication device - it is inherent that code must be stored in the memory in order to execute.

Claims **22 and 23** are rejected under the same reason set forth in connection of claim 18 and 21.

As per **claim 24**, Caputo discloses:

-**generating one time code for the user for the session** (Caputo, col 7, lines 3-7, “The device authentication process is similar to that of message authentication described above, except that a time-varying number 54, such as a random number (or a time and date), is authenticated instead of communications data”), Where “random number” is the one time code, as claimed;

- receiving an authentication datagram from said user (Caputo, col 2, lines 20-25, "transportable authenticating and encrypting device which includes an encryptor for encrypting data received by the device, an authenticator for authenticating use of the device by a user, and a modem for transmitting the data and for receiving the data over a data transfer path"), where "encryption data (self-contained data)" is the Datagram, as claimed;

- passing on said datagram for verification by a remote authentication server if at least an indication of said one time code that matches said user is provided with said datagram (Caputo, col 3, lines 33-37, "The authenticator is preferably a cryptographic means which identifies the authorized user by an authorized user identification such as a message authentication code or digital signature") and (Caputo, col 3, lines 46-49, "Preferably, the compact authenticating and encryption device includes a means of detecting the modification of messages sent or received by message authentication codes or digital signatures"), where "detecting modification message", such as digitally signed and encrypted data used here, as claimed.

Claim 25 is rejected under the same reason set forth in connection of claim 3.

As per **claim 26,** Caputo discloses:

- matching said datagram or a hash of said datagram to a table (Caputo, col 7, lines 30-42, "Digital signatures are a form of authentication which differs from the symmetrical key technology described ... Digital Signature Standard and Secure Hash Algorithm");

-calculating a counter value from a matching position in said table (Caputo, col 7, lines 43-46, "FIG. 5B describes a device and user authentication. In this case, the user's name and, optionally, PIN is signed (Block 71), along with a counter"), where "counter" used, as claimed. Also (Caputo, col 10, lines 2-3, "This ensures that the result will not match if the PIN is incorrect");

- validating said authentication datagram based on an increase in said counter over a previous counter being within a certain limit (Caputo, col 7, lines 43-54, "FIG. 5B describes a device and user authentication. In this case, the user's name and, optionally, PIN is signed (Block 71), along with a counter (or time and date) which indicates that the data sent can be identified as not having been sent previously. The signature is performed using the user's unique private key. The user's name and the signature produced by the X9.30 algorithm are sent (Block 68) to the recipient (Block 66) and verified (Block 65) using the corresponding digital signature verification procedure specified by the standard and a copy of the user's public key. The result of the verification process (Block 65), like the comparison test (Block 64), is a simple pass or fail"), where process of the validating data to check previous use of data used, as claimed.

Claims 27-29 are rejected based on inheritance:

As per **claim 27**, where authentication mechanism based encryption/decryption and it inherently checked or compare for number of try for successful or unsuccessful attempts to identify unwanted visitor.

As per **claims 28-29**, where check for the threshold settings is inherent.

Claim 30 is rejected under the same reason set forth of claim 26 and further "check for the threshold" is inherent.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 9-16, 31-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Caputo et al. (US PAT No. 5546463), hereinafter Caputo and further in view of Douglas S. Daudelin (US PAT No. 4716376), hereinafter Daudelin.

As per **claims 9-16**:

Official notice is hereby taken it is well-known practice of encryption coding, such as using "temporary code", matching user with session ID, using of ActiveX, embedded software, caching data, secure connection between client and server, use of different path for different types of data.

The skilled person would have been motivated to use such algorithm to communicate efficiently and securely in a distributed environment.

As per **claim 31,** Caputo does not teach "detecting a transmission of an acoustic multitone FSK signal**".** However, Daudelin discloses:

- Detecting a transmission of an acoustic multitone FSK signal (Daudelin, col 3, lines 9-10, "FSK demodulator can optimally detect an FSK signal");

- receiving an acoustic signal (Daudelin, col 12, lines, "The constraints stem from the requirement that the received signal pass through the threshold value as the receiver's input frequencies are changed");

- converting the signal into a Hilbert-transform representation of the signal (Daudelin, col 4, lines, "The output of sampling circuit 160 is also applied on line 2 to a fixed phase shifting circuit 170 which includes a Hilbert transformer 4"), where "transformer 4" is the signal converter, as claimed;

- correlating said converted signal with at least one reference signal representing at least one expected frequency in said FSK signal (Daudelin, col 3, lines 48-56, "The demodulator includes a front end band pass filter 101 designed to remove out of band frequency components from an input signal applied on line 100 and supply the filtered signal to a differential detector designated generally at 150 via a sampling circuit 160. The output of demodulator 150 is a d.c. signal plus a double frequency component which is applied to a low pass filter 102 and then to a threshold decision circuit 103"), where "filtered signal" is the converted signal correlating with the "input signal" where "input signal is the original FSK signal, as claimed;

- integrating said correlation over an interval (Daudelin, col 2, lines 29-32, "The 90 degree phase shift at the center frequency is achieved by a constant phase shift circuit which combines the output of a .+-.90 degree phase shifting circuit (advantageously a Hilbert filter) with the output of a scaling circuit having a variable gain factor K"), where, "combining the output" is the integrating and (Daudelin, col 11 , lines 27-32, "The number of counted samples depends upon the expected time interval (period) of each bit of the data signal which modulated the FSK carrier"),over an interval, as claimed;

- determining if a signal is present, based on a shareholding of a result of said integrating (Daudelin, col 13 , lines 45-50, "The difference generated by circuit 504 on line 506 is denominated a "threshold adjusted" signal and is applied to a decision circuit 501 which merely determines whether the threshold adjusted signal is positive or negative. The output from circuit 501 on line 500 represents the original FSK encoded data").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teaching of Caputo with Daudelin's disclosure of transmitting signal from an "authentication card".
The modification would be obvious because one of the ordinary skills in the art would want to have a hacker-proof authentication by using mechanism of transmission of data using frequency shift key.

As per **claim 32**, claim 31 is incorporated and Caputo does teach "detecting signal". However, Daudelin discloses:

- comprising further determining if a detected signal has a frequency within a certain frequency range (Daudelin, col 3, lines 9-13, "FSK demodulator can optimally detect an FSK signal composed of any two frequencies which lie within a broad range of the two frequencies the demodulator is initially tuned to detect").

As per **claim 33**, claim 31 is incorporated and Caputo does not teaches "detecting signal". However, Daudelin discloses:

- determining if a detected signal has a signal to noise ratio within a certain signal to noise ratio range (Daudelin, col 1, lines 31-42, " FSK input signal is formed which is phase shifted an amount that is a function of the instantaneous signal frequency, and the product of the original and phase shifted versions is then computed. The product contains a dc component equal to the cosine of the phase difference between the two signals, and a double frequency component. Ideally, the phase difference is chosen to be 90 degrees at the carrier frequency, in order to permit maximum noise immunity").

The same motivation applies as in claim 31, in this claim 33.

As per **claim 34**, claim 31 is incorporated and further discloses by Daudelin:

- comprising resampling said signal after said determining (Daudelin, col 3, lines 60-62, "The input to detector 150 consists of samples of the filtered FSK signal which are obtained by sampling the output of filter 101").

The same motivation applies as in claim 31, in this claim 34.

As per **claim 35**, claim 31 is incorporated and further discloses by Daudelin:

- wherein said threshold is noise dependent of the received signal (Daudelin, col 4, lines, " This arrangement gives the highest degree of noise immunity and also allows the ensuing threshold decision circuit 103 to operate by simply deciding if the value of the signal output from low pass filter 102 is greater or less than zero").

The same motivation applies as in claim 31, in this claim 35.

As per **claim 36**, claim 31 is incorporated and further discloses by Daudelin:

- calculating said interval based on a hardware characteristic of a producer of said acoustic signal (Daudelin, col 13, lines 66-67, and col 14, lines 1-11, "By virtue of the arrangement of FIG. 5, ... sum of (1) the current threshold and (2) a weighted average of the threshold adjusted signal at a pre selected time after successive (i.e., positive to negative and negative to positive) zero crossings. A typical value for .sigma. would be 1/100 of the maximum value reached by the threshold adjusted signal"), where interval was calculated by the circuit, as claimed.

The same motivation applies as in claim 31, in this claim 36.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see form "PTO-892 Notice of Reference Cited").

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Monjour Rahim whose telephone number is (571)270-3890. The examiner can normally be reached on 6:00 AM - 4:00 PM (M - TH).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chameli Das can be reached on (571)272-3696. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Monjour Rahim
Patent Examiner
Art Unit 4141
Date: 03/04/2008

/CHAMELI C. DAS/

Supervisory Patent Examiner, Art Unit 4141